2017 年 6 月 28 日

標準ログサーバー設定

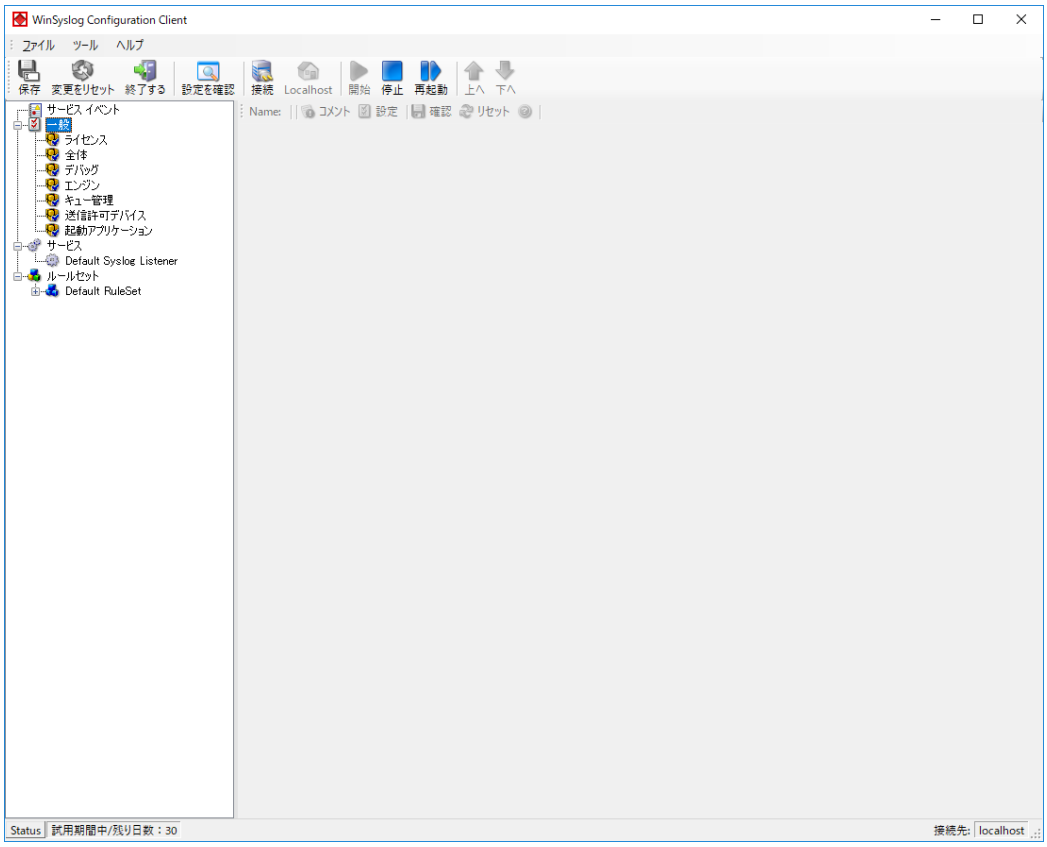
最も標準的なログサーバー機能を設定します。
シスログを UDP/514 で受信するよう設定していることを確認し、受信したログの全てをテキストファイルに保存するように設定を追加します。
※WinSyslog ver.14.1～ インストール直後の初期設定が変更され、ファイルログアクションはデフォルトルールに追加されています。
（日本国内ユーザー向けのため弊社からダウンロードしたインストーラのみ）
ファイルログアクションを追加する手順はスキップし、追加後の詳細設定よりご参照ください。

1　設定プログラムを起動します

ここでは、新クライアントの場合で説明します。（旧バージョンのクライアントを使用する場合は、WinSyslog Leagcy Client を起動します。）
アプリケーション一覧より WinSyslog Configuration をダブルクリックします。

（C:¥Program Files (x86)¥ WINSyslogClient.exe）

設定クライアント(WinSyslog Configuration Client）が起動します。

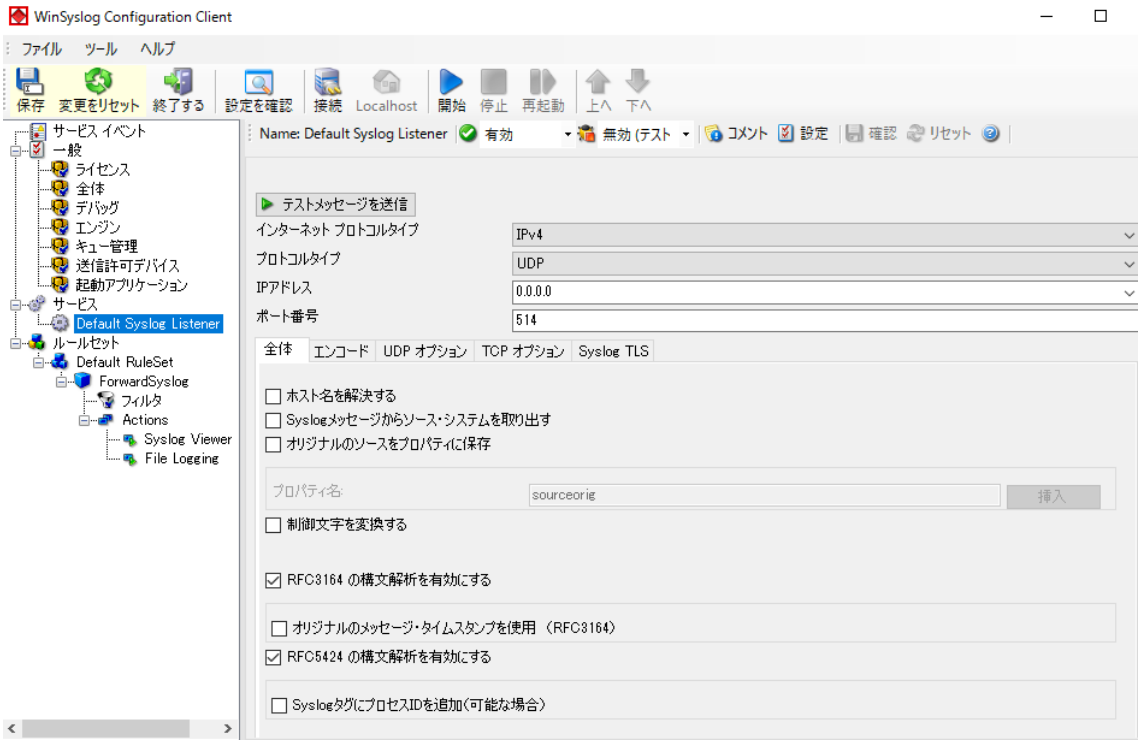


注意 ： この GUI が英語表示の場合は、以下の手順で日本語に変更してください。
http://www.jtc-i.co.jp/support/documents/etc/winsyslog_language_setting.pdf

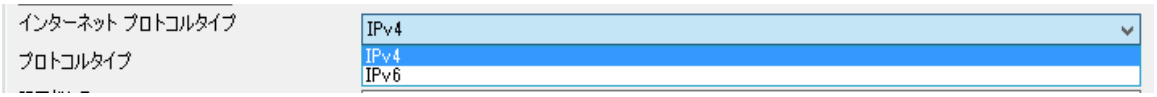
2 既存サービスの確認

左ペインのツリーで、サービス> Default Syslog Listener を選択します。
このサービス内に、「Syslog サーバー」、「SNMP トラップ受信」、そして、ハートビートなどの用途別のサービスを追加することができます。

ここでは、既存の”Default Syslog Listener”の主な内容を確認します。

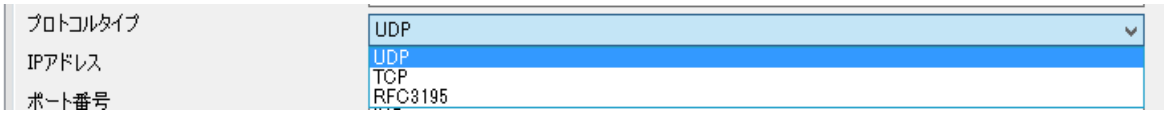


1. 右ペイン表示で、インターネットプロトコルタイプのプルダウンを開くと、選択肢として、IPv4/IPv6 の選択が可能です。デフォルトは、IPv4 です。



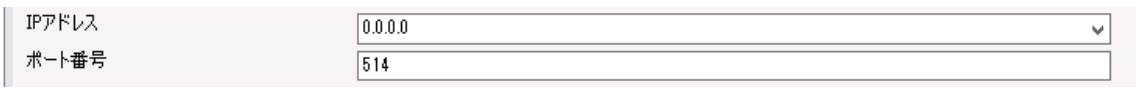
注記：IPv6 も設定したい場合は、サービスを別に追加してください。

2. プロトコルタイプとして、UDP/TCP/RFC3195 の選択肢があります。デフォルトは UDP です。



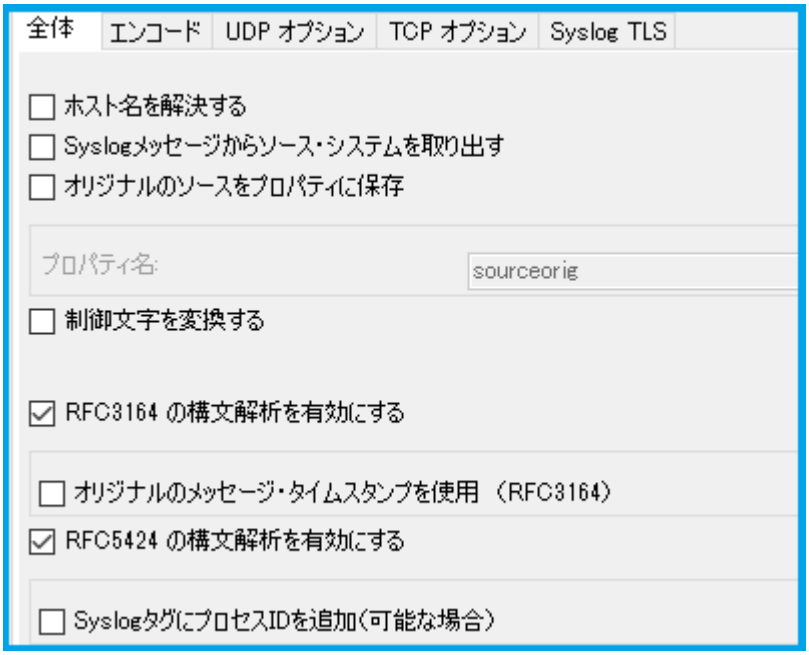
3. IP アドレスとして、デフォルトでは、0.0.0.0 が指定されており、これは、全ての IP アドレスを意味します。（複数 NIC を持つ場合は、特定の IP アドレスを指定すると、そのアドレスで受信した Syslog のみ処理されます）

ポート番号として、514 がデフォルトとして設定されています。



4. 以下のタブは必要に応じて設定します。

4-1. 全体



□ホスト名を解決する

これを有効にすると、DNS サーバーの名前解決機能を使用します。無効の場合は、IP アドレスを使用します。

※以下の「Syslog メッセージからソース・システムを取り出す」オプションが有効の場合、Syslog メッセージからの情報が優先されます。

□Syslog メッセージからソース・システムを取り出す

これを有効にすると、RFC3164 に由来するシスログメッセージからソース情報を取り出して使用します。RFC3164 に準拠しないデバイスが多くある場合は、正しい情報が表示されない場合があります。

□オリジナルのソースをプロパティに保存

これを有効にすると、オリジナルの送信元情報が指定したプロパティ(デフォルトでは %sourceorig%)に保存されます。このプロパティの値でフィルタをかけたい場合に便利です。

□制御文字を変換する

これを有効にすると、制御文字が含まれている場合、ASCII 文字 ID に置き換えます。2 バイト文字セットを使用している場合は、文字化けの原因となるのでチェックを外します。

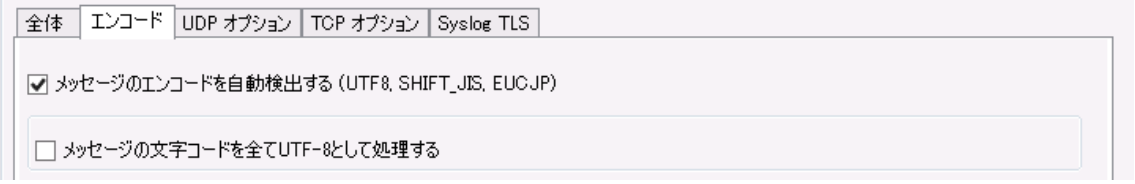
□RFC3164 の構文解析を有効にする:RFC3164 に対応したメッセージの構文解析が可能

送信元やタイムスタンプが正常に処理されない場合は、チェックを外してください。

□オリジナルのメッセージ・タイムスタンプを使用 （RFC3164）
これを有効にすると、RFC3164 に由来するシスログメッセージが持つタイムスタンプが使用されます。異なるタイムゾーンのデバイスが複数ある場合は、チェックを外すことをお勧めします。

□RFC5424 の構文解析を有効にする：RFC5424 に対応したメッセージの構文解析が可能
送信元やタイムスタンプが正常に処理されない場合は、チェックを外してください。

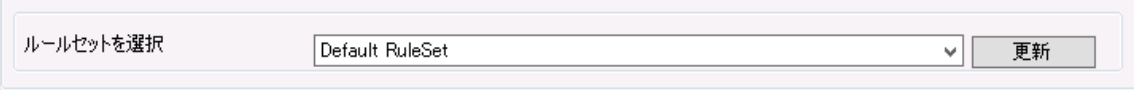
4-2. エンコード
エンコードタブでは、デフォルトで以下のように、
□メッセージのエンコードを自動検出する(UTF-8, SHIFT_JIS, EUCJP)
のオプションにチェックが入っています。



注記：メッセージに2バイト文字が含まれる場合、内部処理で自動的に UTF16 に変換されますので、注意が必要です。

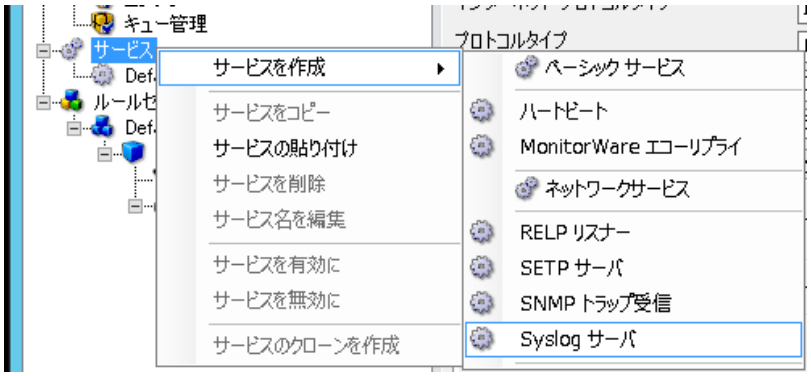
□メッセージの文字コードを全て UTF-8 として処理する
これを有効にすると、BOM がついていないシスログメッセージを BOM 付で処理します。
UTF-8 以外のエンコードメッセージは正しく処理されませんのでご注意ください。

5. 全体タブ最下の「ルールセットを選択」で、このサービスで実行するルールセットを選択します。
デフォルトでは、Default RuleSet のみがルールセットとして設定されています。
変更した場合は、「更新」ボタンをクリックします。

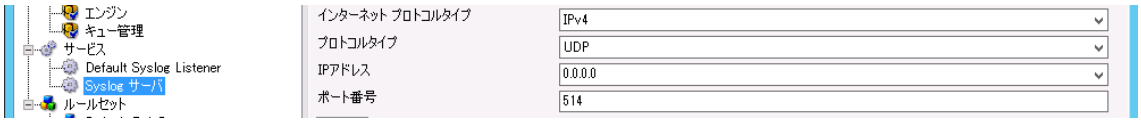


3 サービスの追加

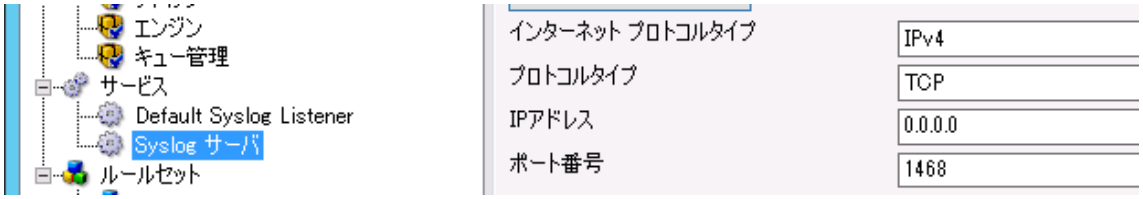
新たにサービスを追加するには、左ペインで「サービス」を右クリックし、「サービスの追加」を選択します。Syslog サーバーを追加する場合は、サブメニューから、「Syslog サーバー」を選択します。



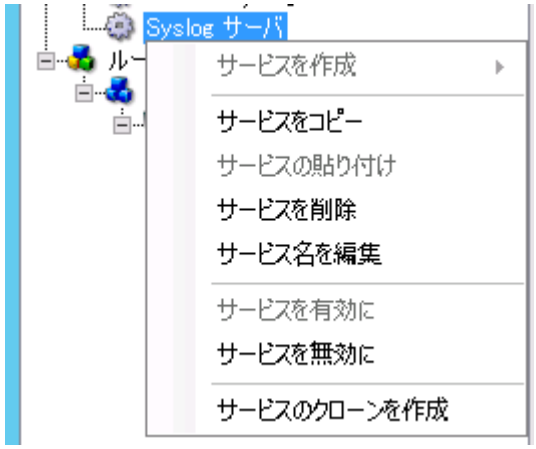
左ペインに「Syslog サーバー」が追加され、その内容を示す右ペインではデフォルトルールが表示されています。適切な設定に変更してください。



例：TCP/1468 用



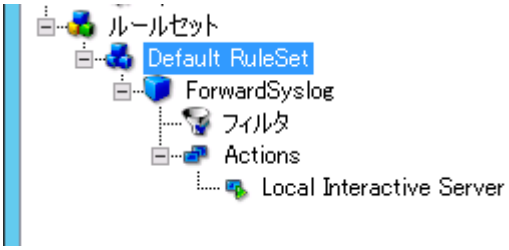
「サービス」のコピー、削除、名称変更などは、左ペインで当該の「サービス」を右クリックすると、メニューが表示されます。



4　ルールセットの内容確認とファイル保存のアクションを追加

インストール後のデフォルトのルールセットのツリーには、「Default RuleSet」1つのみ設定されています。

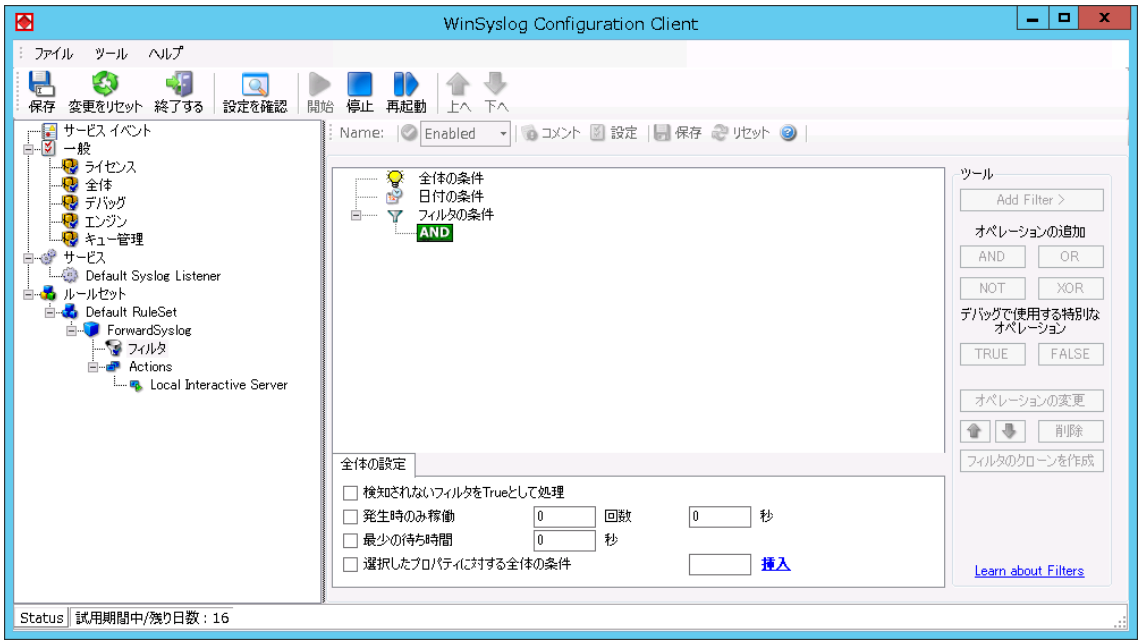
注記：サービス（受信リスナー）ごとに1つのルールセットを指定しますので、適用するルールセットを変更したい場合は、ルールセットを追加します。



「Default RuleSet」内のツリーを確認します。

「ForwardSyslog」というルールがあります。

「ForwardSyslog」>フィルタをクリックして、右ペインを表示します。

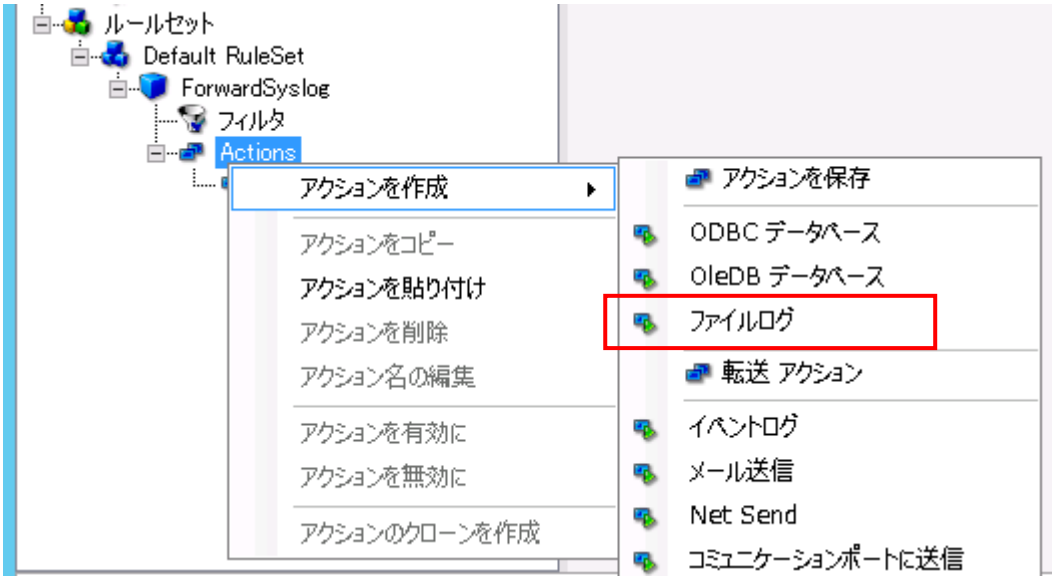


デフォルトでは、フィルタ条件がありませんので、すべての受信ログを無条件で処理します。

※WinSyslog ver.14.0 以前のバージョンの場合：ファイルログアクションを追加します。

「Default RuleSet」>「ForwardSyslog」>「Actions」を右クリックし、

サブメニューから「アクションを作成」>「ファイルログ」を選択します。



※ WinSyslog ver.14.1～は、インストール直後の初期設定でファイルログアクションが既に追加されていますので、次のステップから、ご確認ください。

右ペイン「ファイル名に関するオプション」項目では、以下の設定になっています。

デフォルト設定は、以下の通りです。

出力エンコード：システムデフォルト

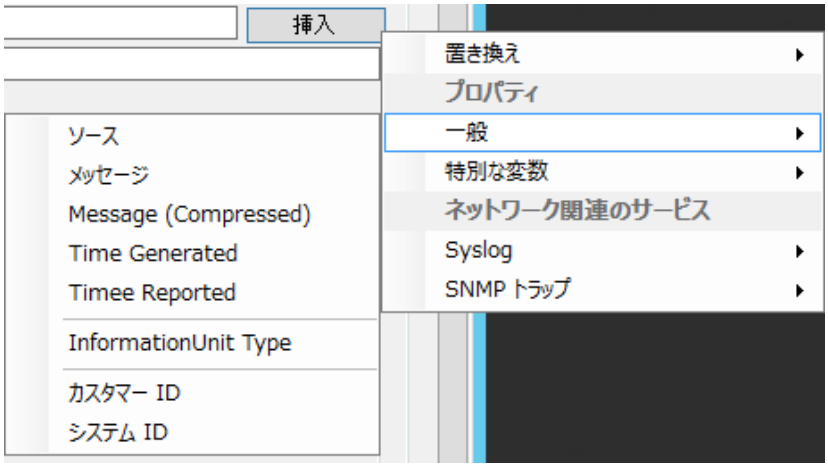
ファイルパス： C:¥Program Files (x86)¥WinSyslog

ファイルベース名： WinSyslog
ファイル拡張子： log
⊙ローテーションを無効にする
☑ファイル名に日付を出力

上記の場合、C:¥Program Files (x86)¥WinSyslog フォルダ下に、
WinSyslog-2016-04-11.log
WinSyslog-2016-04-12.log
のように、毎日ファイルが作成されることになります。

ログを保存するフォルダを変更する場合は、「ファイルパス」の「参照」ボタンをクリックし、フォルダを選択します。（パス名に存在しないフォルダ名を指定しても自動でフォルダは作成されません）

ファイルベース名： WinSyslog にプロパティ（変数）を挿入して自動でソースの IP アドレスやプライオリティなどを付与するなどの設定も可能です。
「挿入」タブをクリックすると自動で付加できる変数が選択できます。



例 1）ソース名（送信元）を付加したフォルダ名で分割し、ファイル名にもソース名を入れる場合
ファイルパス：**F:¥syslogs¥%source%**
ファイルベース名：**IIS-%source%**
と設定すると、ソース IP が 10.0.0.1 の場合、ファイル名は以下のようになります。
F:¥syslogs¥10.0.0.1¥IIS-10.0.0.1.log

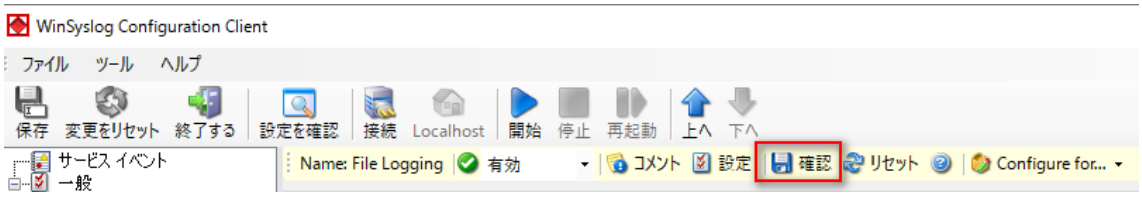
例 2）ファイルを日時（日付と時間）情報で分割する場合
ファイル名：**Syslog-%timegenerated:1:10%_%timegenerated:12:13%**

と設定すると、ファイル名は **Syslog-2016-4-12_05.log** のようになります。

注記：**%timegenerated%**(生成時刻)および**%timereported%**(報告時刻)のプロパティを使用する際、UTC 時刻(-9 時間)が適用されます。ローカルタイムで表示したい場合は、**%timegenerated:12:13:localtime%** のように入力します。

「ファイルフォーマット」項目では、以下の設定になっています。
デフォルトでは、「Adiscon」フォーマットが選択されており、その下のオプションにおいて、チェックした情報が出力されます。

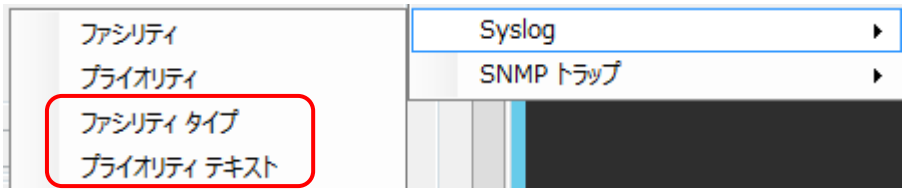
設定を変更すると、右ペイン上部の「確認」アイコンが選択できるように表示が変化します。
「確認」アイコンをクリックすると、設定は一時保存され、他の画面に移行できます。



※ver.13.1 以前は、この「確認」は「保存」ボタンでした。

〇カスタムフォーマット を選択すると、出力するプロパティの順序や区切り文字をカスタマイズすることができます。

例） Syslog ファシリティと Syslog プライオリティ（Severity）を数ではなく文字で出力したい場合：
ファシリティタイプ(%syslogfacility_text%)、プライオリティテキスト(%syslogpriority_text%)を選択すると、Local6,Informational のように出力されます。



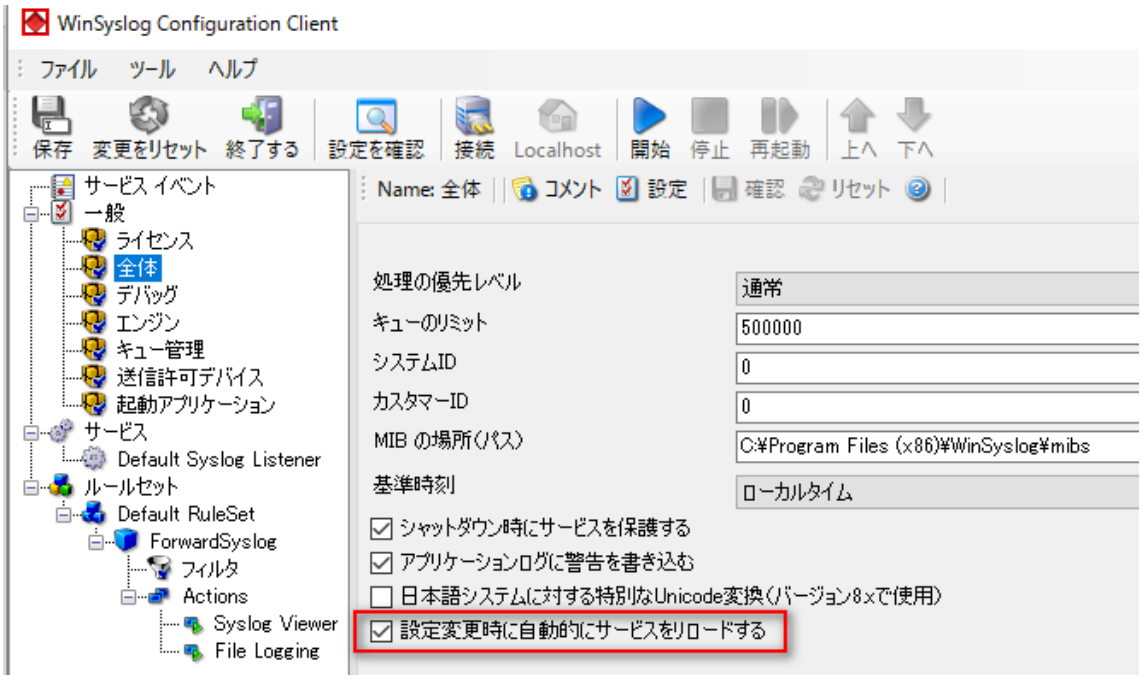
5 サービス再起動（設定の反映）

WinSyslog ver.14.0 以前のバージョンでは、WinSyslog は設定変更をダイナミックに読んで反映することはありません。設定変更後はサービス再起動が必要です。

設定変更後、トップメニュー下の「保存」→「再起動」をクリックします。

サービス再起動後、新たな設定が有効になり、受信ログが処理されます。

WinSyslog ver.14.1～ 「設定変更時に自動的にサービスをリロードする」オプションが追加となりました。
このオプションはデフォルト設定では有効ですので、設定変更後「保存」ボタンのみで変更が反映されます。
この機能を無効にしたい場合は、チェックを外してください。


WinSyslog Configuration Client
ファイル
ツール
ヘルプ
保存
変更をリセット
終了する
設定を確認
接続
Localhost
開始
停止
再起動
上へ
下へ
サービス イベント
一般
ライセンス
全体
デバッグ
エンジン
キュー管理
送信許可デバイス
起動アプリケーション
サービス
Default Syslog Listener
ルールセット
Default RuleSet
ForwardSyslog
フィルタ
Actions
Syslog Viewer
File Logging
Name: 全体
コメント
設定
確認
リセット
処理の優先レベル
通常
キューのリミット
500000
システムID
0
カスタマーID
0
MIB の場所(パス)
C:¥Program Files (x86)¥WinSyslog¥mibs
基準時刻
ローカルタイム
シャットダウン時にサービスを保護する
アプリケーションログに警告を書き込む
日本語システムに対する特別なUnicode変換(バージョン8xで使用)
設定変更時に自動的にサービスをリロードする

以上